使用CUWN解决无线客户端互操作性问题

目录

简介
先决条件
要求
使用的组件
背景信息
一、问题定义
二。 WLC配置和一般日志
运行配置
WLC配置文件
GUI
CLI
来自WLC的系统日志
三。客户端设备详细信息和信息
四。网络拓扑
V.跟踪其他详细信息和具体信息
六。 WLC - Show和Debug命令
WLC Debug命令
WLC Show命令
七。 AP - Show和Debug命令
轻量Cisco IOS®接入点
AP Show命令
AP调试命令
AP-COS接入点
AP-COS Show命令
1800 系列 | AP-COS调试命令
2800/3800系列 | AP-COS调试命令
八。客户端数据包捕获
九。空中(OTA)数据包捕获
802.11n捕获
802.11ac OTA捕获
十。总结
一、问题定义
二。 WLC配置和日志
三、客户端设备信息
四。网络拓扑图
V.创建电子表格记录所有客户问题
VI. WLC上的Show和Debug命令
七.AP上的show和debug命令
轻量Cisco IOS® AP
AP-COS AP

八、客户端捕获
九。技术咨询小组
802.11n捕获
802.11ac捕获
十一。附录A — 其他提示和诀窍
Windows 窗口版本
macOS（以前称为OS X）

简介

本文档介绍思科统一无线网络(CUWN)解决方案出现时的互操作性问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科无线AP
- 无线LAN控制器(WLC)
- 相关网络设备

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

> **注意**：本文档的目标读者是经验丰富的无线网络工程师和管理员，他们已熟悉这些主题的使用、配置和故障排除。

背景信息

经常会发现，给定了各种既存在又继续被开发客户端设备。在建立、维护或仅充分利用与无线网络的连接和支持基础设施方面可能会出现各种问题。

这通常可以归结为客户端设备和/或无线基础设施本身的简单配置问题。但是，在某些情况下，这可以归因于与特定客户端设备和支持它的组件（请求方、WLAN适配器、无线驱动程序……）和/或所涉AP相关的互操作性问题。作为无线工程师，此类互操作性问题为识别、排除和解决潜在的复杂挑战提供了机会。

本文档详细描述了在思科统一无线网络(CUWN)解决方案出现此类无线互操作性问题时，需要初步收集哪些信息来有效地调查和解决这些问题。随着无线客户端设备和接入点(AP)无线电的数量和组合不断增加，对此类全面方法的需求也变得越来越重要。鉴于可能规定此类要求的变量数量不限，可能需要逐个收集有关本文概述内容的更多信息。但是，此处详述的信息是解决任何潜在无线客户端互操作性问题的通用指南。

一、问题定义

要想有效地处理任何问题，并打算采取果断措施，第一步是准确界定相关问题。为此，请确保至少提出以下问题并清楚地记录其答案：

- 此问题是否仅限于AP和/或无线电类型的特定型号（2.4 GHz与5 GHz）？
- 是否仅在特定版本的WLC软件上观察到此问题？
- 仅客户端类型和/或软件（操作系统版本、WLAN驱动程序版本……）的特定版本遇到的问题
- 是否有其它无线设备不存在此问题？如果有，是什么问题？
- 当客户端连接到一个简化的无线设置（例如信道宽度为20 MHz、禁用802.11ac的开放式SSID）时，该问题是否可以重复出现？（即，问题是否只发生在802.11n模式与仅802.11ac模式上？）。
- 如果问题在开放式SSID下无法再现，则至少会发现什么安全配置？（WLAN上的PSK或802.1X）。
- 以前已知良好的配置和软件版本是什么？

二。 WLC配置和一般日志

运行配置

无一例外，绝对有必要收集WLC配置，以详细查看客户使用的功能、其特定设置以及其他此类详细信息。为此，您必须建立到有问题的WLC的Telnet/SSH会话，并将这些CLI命令的输出保存到文本文件：

```
config paging disable

show run-config
```

始终优先选择完整的运行配置输出，因为它包括与加入的AP相关的详细信息以及相关的RF信息。但在某些情况下和情况下，例如最初使用加入大量AP的WLC（8510 WLC和2500多个AP）。可能最好最初只收集WLC的配置，而不收集此类AP信息，以便快速查看，因为完整的show run-config可能需要30分钟或更长时间才能完成给定数量的AP。但是，以后可能仍需要收集完整的run-config输出。

为此，您可以选择将以下CLI命令的输出收集到文本文件：

```
config paging disable

show run-config no-ap

show wlan apgroups
```

WLC配置文件

除show run-config或show run-config no-ap输出外，还建议收集WLC配置的完整备份。如果实验室重建需要由TAC/HTTS和BU升级共同进行，则这有助于在思科实验室环境中尝试重现问题。可以通过相关WLC的GUI或CLI收集WLC的备份，并使用TFTP或FTP将配置文件保存到外部TFTP/FTP服务器。本示例展示使用TFTP使用GUI和CLI保存WLC的备份：

GUI

命令>上传文件>配置>上传，如图所示。

CLI

```
transfer upload datatype config

transfer upload mode tftp transfer upload serverip <TFTP-Server_IP-address> transfer upload path
/ transfer upload filename <desired-filename> transfer upload start
```

来自WLC的系统日志

此时，您还希望从WLC收集当前日志，以便根据需要进行其他检查。理想情况下，您希望在测试后立即通过无线客户端收集这些日志，从而重现报告的问题。如果客户将WLC日志导出到外部系统日志服务器，则您需要从该服务器检索这些日志。否则，通过将此CLI会话输出保存到其他文本文件，可以保存当前本地存储在WLC上的msglog和traplog:

```
config paging disable

show msglog

show traplog
```

三。客户端设备详细信息和信息

下一步是收集尽可能多的有关正在使用的客户端设备的信息和细节，这些设备可能会遇到潜在的无线互操作性问题。此类信息必须包括（但不一定限于）以下内容：

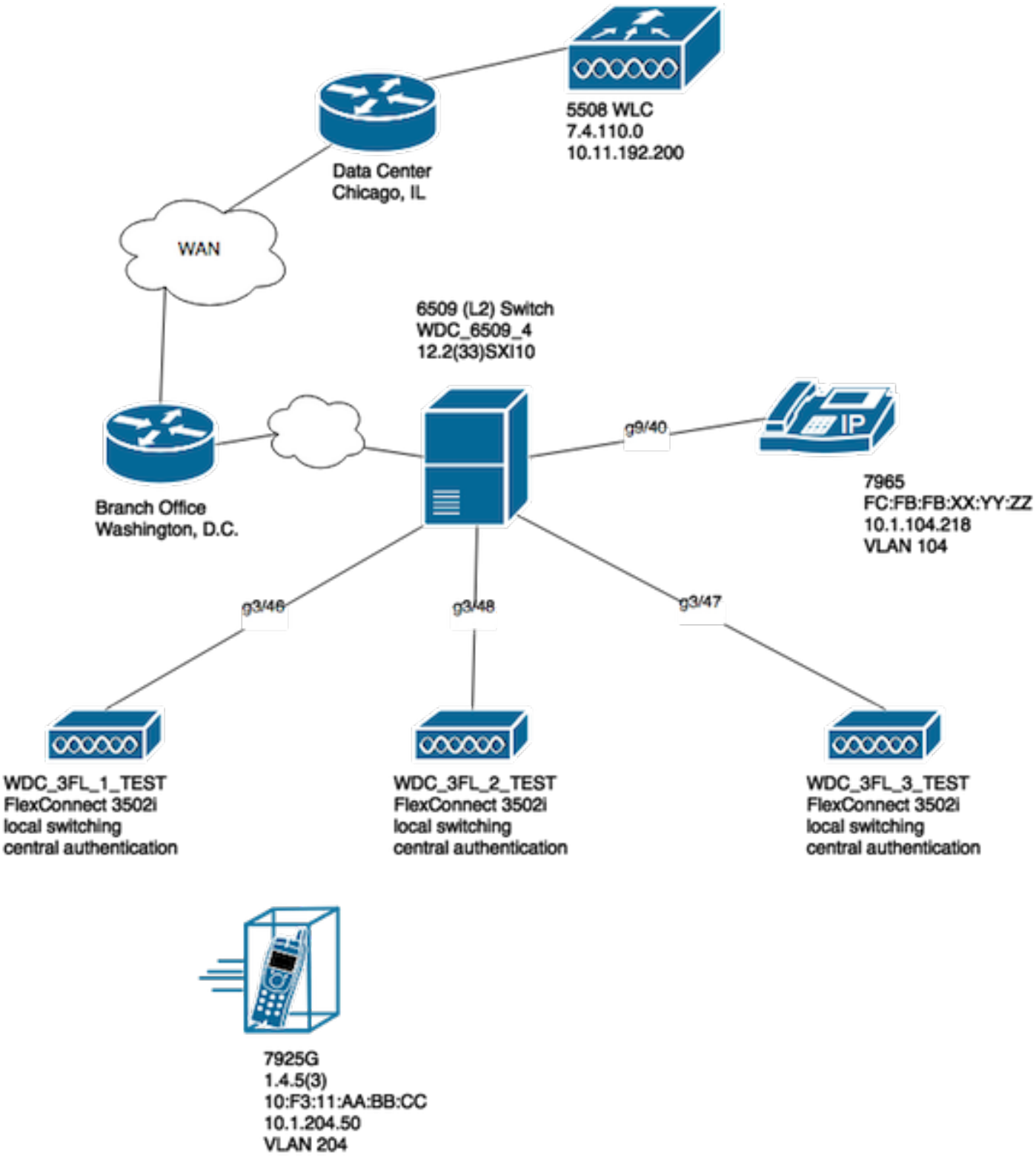
- 客户端类型（平板电脑、智能手机、笔记本电脑……）
- 设备的品牌和型号
- 操作系统 版本
- WLAN适配器型号
- WLAN适配器驱动程序版本
- 使用的请求方（Windows零配置/自动配置、英特尔PROSet...）
- 为无线客户端和WLAN(Open、PSK、EAP-PEAP/MSCHAPv2、...)使用配置的安全性
- 请注意已从相关供应商提供的默认设置（睡眠状态、漫游参数、U-APSD、...）更改的所有客户端参数。

注意：有关客户端设备的任何其他信息或说明，包括其WLAN相关配置的屏幕截图等，也必须根据需要提供。

四。网络拓扑

为进一步加快故障排除工作和根本原因分析(RCA)流程，我们始终建议提供详细而全面的网络拓扑图。网络拓扑图不仅必须包含有关网络和无线基础架构的详细信息，还必须提供对问题无线设备（打印机/扫描仪、正在使用哪些客户端VLAN...）及其相对位置的深入了解。

可以使用许多工具(Microsoft Visio、draw.io、...)和各种样式来创建这样的网络图。重要方面是确保正确的信息清楚地反映在供所有相关方和供应商查看的图表中。示例网络拓扑，捕获有关基础设施和客户端设备的基本但有用的信息，如图所示。



V.跟踪其他详细信息和具体信息

帮助确保在对最终用户遇到问题的客户端设备进行任何测试时收集适当的信息。建议预先创建一个电子表格或类似文件，以记录测试时观察到的所有客户端问题及相关详细信息，例如以下示例：

Mac 地址	用户名	所报告症状的描述	最终用户观察到症状的时间	Ping默认网关
xxyy.aabb.0011	test_user1	间歇性断开与接入点的连接。	从AP3丢失网络连接和无线关联。	n

本练习的目标是帮助记录和确定共同感兴趣的模式，以及准确了解当前的问题。一旦准备使用此电子表格进行数据收集，您就可以开始测试了。下面列出了一些其他但重要的注意事项：

> **注意**：收集的所有调试和数据包捕获需要同步到同一NTP服务器，以便更轻松地与日志关联，并且必须同时执行任何给定测试。
>
> **注意**：提供观察问题的时间以及问题似乎可以恢复的时间（如果适用）的准确时间戳。
>
> **注意**：始终收集AP和WLC上按客户端MAC地址过滤的调试。
>
> **注意**：不要在同一Telnet/SSH/控制台会话内的AP上运行show和debug命令，这些命令会在不同的会话中分别执行。
>
> **注意**：AP调试优先于Telnet/SSH与控制台进行，因为控制台通常速度太慢，无法生效。

六。 WLC - Show和Debug命令

在进行测试以重现潜在的无线客户端互操作性问题并排除其故障时，必须从正在使用的无线基础架构中收集调试和额外日志。这两个部分可以详细解释分别从WLC和AP收集的特定日志和初始调试输出。

WLC Debug命令

```
config sessions timeout 0
debug client <MAC_address> debug dhcp message enable
```

关于当前问题的性质，您还可以逐个案例添加以下WLC调试：

- **debug aaa detail enable** — 如果AAA服务器存在身份验证相关问题，请使用此命令
- **debug aaa events enable** — 如果AAA服务器存在身份验证相关问题，请使用此命令
- **debug aaa all enable** — 将此命令用于身份验证问题；此调试的输出是详细的，因此仅在绝对

需要时使用（对于AAA覆盖情况，..）
- **debug mobility handoff** — 当WLC之间出现漫游问题时使用

问题重现至涉及的无线客户端后，系统将收集和记录之前和之后各部分中概述的所有信息。要执行这些CLI命令，您必须禁用WLC上的调试。

```
debug disable-all
```

WLC Show命令

```
config paging disable

show time

show client detail <MAC_address>

ping <client_IP-address> <repeat count [1-100]>
```

如前所述，确保在一个Telnet/SSH会话中运行WLC调试，并在另一个通向WLC的Telnet/SSH中收集这些show命令的输出。您必须执行相同的操作以收集本节中详细介绍的AP调试和show命令输出。

七。 AP - Show和Debug命令

轻量Cisco IOS®接入点

在开始任何参与测试的轻量Cisco IOS® AP（如2600、2700、3700或之前型号的Cisco接入点）上进行任何调试之前。您必须首先在AP上执行以下CLI命令，以避免在客户端测试时Telnet/SSH/控制台会话到相关AP时超时：

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

您也可以按照以下步骤使用控制台连接，并将**line vty 0 4**语句替换为**line console 0**，以便相应地禁用串行/控制台连接的exec和会话超时。

- line console 0 — 用于修改串行会话超时参数
- line vty 0 4 — 用于修改Telnet/SSH会话超时参数

AP Show命令

在开始测试之前，您必须首先在AP上收集这些show命令的示例。在测试完成之前和之后，针对涉及相关无线客户端的每个测试，至少收集两次show命令的输出。

```
term len 0
```

```
show clock

show tech

show capwap client mn

show int do1 dfs

show logging

more event.log

show trace dot11_rst display time format local

show trace dot11_rst

show trace dot11_bcn display time format local

show trace dot11_bcn
```

AP调试命令

收集上述show命令的初始输出后，您现在可以在单独的Telnet/SSH会话中在同一接入点上启用调试，如下所示。确保将整个输出保存到文本文件。

```
debug dot11 {d0|d1} monitor addr <client_MAC-address>

debug dot11 {d0|d1} trace print clients mgmt keys rxev txev rcv xmt txfail ba

term mon
```

标志	描述
d0	2.4 GHz射频（插槽0）
d1	5 GHz射频（插槽1）
管理	跟踪管理数据包
ba	跟踪块ACK信息
rcv	跟踪接收的数据包
密钥	跟踪设置密钥
rxev	跟踪已接收的事件
txev	跟踪传输事件
txrad	跟踪传输到无线电
xmt	跟踪传输数据包
txfail	跟踪传输故障
速率	跟踪速率更改

要在完成测试和数据收集过程后禁用AP上的调试，可以在AP上执行以下CLI命令：

```
u all
```

AP-COS接入点

适用于支持802.11ac第2波接入点和更高版本的接入点，例如1800、2800和3800型号接入点。这些较新的型号AP为称为AP-COS的接入点平台引入了一种全新的操作系统。因此，以前详述的传统轻量级基于Cisco IOS®的接入点上使用的所有命令仍然适用。如果排除故障时涉及与各种客户端STA设备和AP-COS型号AP的互操作性问题，则必须从与等效测试相关的AP-COS接入点收集这些信息。

在测试所涉及的任何AP-COS型号AP上启动任何调试之前。您必须首先在AP上执行以下CLI命令，以避免在客户端测试时Telnet/SSH/控制台会话到相关AP时超时：

```
exec-timeout 0
```

AP-COS Show命令

在开始测试之前，您必须首先在AP上收集这些show命令的示例。在测试完成之前和之后，针对涉及相关无线客户端的每个测试，至少收集两次show命令的输出。

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

1800 系列 | AP-COS调试命令

这些调试特定于18xx系列接入点。这是因为用于1800系列AP的芯片组与2800/3800系列接入点中的芯片组不同，因此本场景需要一组不同的调试。下一节将介绍2800/3800系列AP的相应调试。

收集上述show命令的初始输出后，您现在必须在单独的Telnet/SSH会话中启用相同1800接入点上的调试，如下所示。确保将整个输出保存到文本文件。

```
debug dot11 client level events addr <client_MAC-address>

debug dot11 client level errors addr <client_MAC-address>

debug dot11 client level critical addr <client_MAC-address>

debug dot11 client level info addr <client_MAC-address>

debug dot11 client datapath eapol addr <client_MAC-address>

debug dot11 client datapath dhcp addr <client_MAC-address>

debug dot11 client datapath arp addr <client_MAC-address>
```

在某些情况下，您可能还需要在18xx AP上启用其他调试，以进一步排除客户端互操作性问题。但是，只有当/根据思科TAC工程师对相应服务请求/案例的请求，才应执行此操作。

因为额外的调试不仅在其输出中更为冗长，而且还会在AP上引入额外的负载，因此它需要额外的时间进行适当的分析。如果许多客户端设备尝试连接到测试中的同一AP或类似的变量，在某些情况下可能会中断服务。

要在AP-COS变体接入点上禁用调试（无论是在1800或2800/3800系列AP上），完成测试和数据收集过程后，可以在AP上执行以下CLI命令：

```
config ap client-trace stop
```

2800/3800系列 | AP-COS调试命令

收集上述show命令的初始输出后，您现在必须在单独的Telnet/SSH会话中启用相同2800/3800接入点上的调试，如下所示。确保将整个输出保存到文本文件。

```
config ap client-trace address add <client_MAC-address>
config ap client-trace filter all enable
config ap client-trace output console-log enable
config ap client-trace start
term mon
```

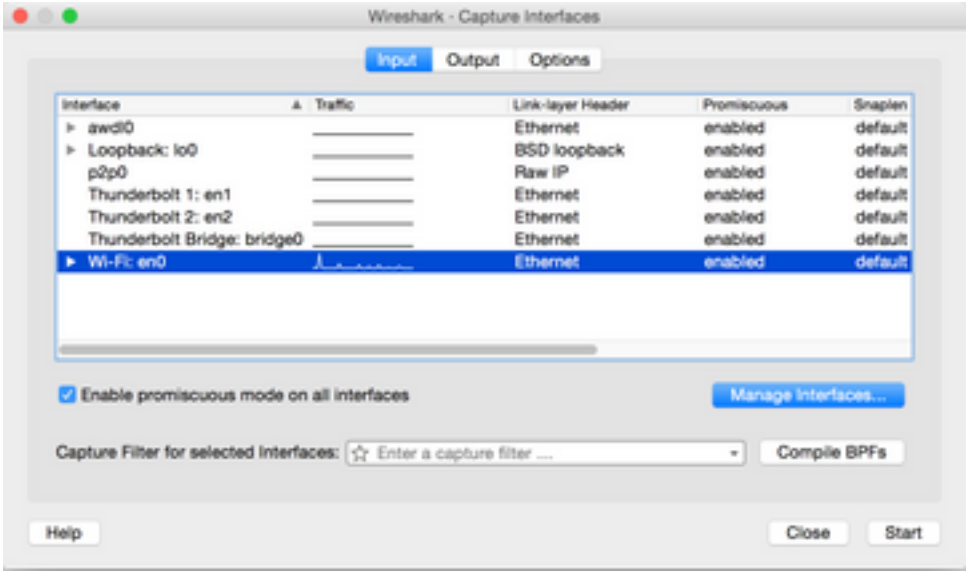
要在完成测试和数据收集过程后禁用1800/2800/3800系列AP上的调试，可以在AP上执行以下CLI命令：

```
config ap client-trace stop
```

八。客户端数据包捕获

从正在使用的客户端设备（如果是笔记本电脑、MacBook或类似设备），必须从用于重现问题的客户端设备的无线接口收集混杂模式数据包捕获。Netmon 3.4（仅Windows）或Wireshark等常用工具可以轻松下载并用于收集此捕获并将其保存到*.pcap文件。取决于设备，可能还有方法从相关客户端收集tcpdump或类似信息，因此您可能需要咨询客户端设备制造商以获得这方面的帮助。

以下示例为MacBook Pro上的无线接口配置Wireshark捕获：



与任何数据包捕获一样，无论使用什么实用程序收集数据包，请确保以pcap文件格式(*.pcap，*.pcap， *.pkt，...)保存文件。这样做是为了确保不仅任何部门的思科工程师都可以轻松查看数据包捕获文件，其他供应商和组织（英特尔、苹果、.....）的工程师也能轻松查看。这样可以实现更加无缝的合作和协作流程，从而进一步促进思科和客户端设备供应商更好地合作，以调查和解决任何潜在的互操作性问题。

九。空中(OTA)数据包捕获

为了有效排除任何潜在的或现有的无线互操作性问题，收集高质量的OTA数据包捕获问题至关重要。这允许详细分析无线客户端和无线接入点无线电之间的实际802.11无线通信，此外还提供客户端

和无线基础设施日志以及调试的进一步视角。这是对潜在无线互操作性问题的每项测试都无一例外地必须完成的关键步骤。

但是，终端客户往往没有适当装备或准备收集OTA数据包捕获。这是无线工程师经常遇到的常见障碍，他们必须与客户合作以多种方式克服这一障碍。思科支持论坛上的这篇文章可以作为良好的开端，帮助指导并相应培训客户：

802.11无线嗅探/数据包捕获

OTA数据包捕获必须以pcap文件格式(*.pcap， *.pcap， *.pkt，...)收集，并包括802.11元数据（RSSI、信道、数据速率，..）。在测试期间，OTA嗅探器还必须始终紧邻相关客户端设备，以确保准确观察发送和接收到/来自所测试客户端设备的流量。

> **注**意：如果相关测试涉及客户端设备漫游场景，需要在聚合数据包捕获中监控多个802.11信道。因此，目前不建议使用Fluke Networks的AirMagnet WiFi Analyzer。

原因在于，使用此实用程序的聚合数据包捕获当前以专有文件格式保存，而不是在Wireshark或其他类似实用程序中易于查看的pcap样式格式。确保您的OTA数据包捕获采用非专有文件格式，这有助于确保所有相关方和供应商能够随时查看任何捕获文件，最终帮助加快任何解决工作。

采用当前Wireshark可读取的格式，包括802.11元数据（RSSI、信道、数据速率）— 有关详细信息，请访问： https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
以下是一些收集OTA数据包捕获的常用方法：

- 带Wireshark的AirPCAP
- MacBook Pro
- OmniPeek Professional、OmniPeek Enterprise、...
- OmniPeek远程助理(ORA)
- 嗅探器模式下的思科AP

802.11n捕获

对于涉及802.11n无线客户端的OTA数据包捕获，目前具有更大的灵活性和易用性。这是因为有更多的可用无线USB WLAN适配器可以很容易地与许多工具（如OmniPeek和其他工具）配合使用。

请注意用于收集802.11n OTA捕获的特定无线适配器的功能与您尝试进行故障排除的客户端设备使用的实际WLAN芯片组的功能有何异同。例如，如果客户端设备遇到使用支持2空间流(2SS)的802.11n芯片组的潜在无线互操作性问题。然后，强烈建议确保用于收集OTA数据包捕获的无线适配器也是2SS或更好的适配器，具有802.11n或更高规格。

802.11ac OTA捕获

对于3空间流(3SS)802.11ac捕获，您可以使用2014型号MacBook Pro或更高版本以及Mac OS X 10.10.x或更高版本的本机嗅探功能。如果对2空间流802.11ac客户端设备进行故障排除，您还可以使用MacBook Air进行802.11ac捕获。MacBooks的Air型号目前仅使用2SS WLAN芯片组。有关如何使用Mac OS X通过各种方法收集OTA数据包捕获的说明，请参阅列出的思科支持论坛文章：

使用Mac OS X 10.6+进行无线嗅探

您也可以在嗅探器模式下使用2702/2802/3702/3802系列或类似的AP来收集使用3SS的适当802.11ac数据包捕获。您也可以参阅列出的资源，查看当前可用的802.11ac无线适配器列表。其中一些可以与OmniPeek等常用工具一起使用，以及其他工具来收集802.11ac数据包捕获（来自Ralink、Atheros的芯片组……）：

https://wikidevi.com/wiki/List_of_802.11ac_Hardware#Wireless_adapters

您也可以在嗅探器模式下使用2702/2802/3702/3802系列或类似的AP来收集使用3SS的适当802.11ac数据包捕获。为方便起见，有关如何在嗅探器模式下配置思科AP并收集OTA数据包捕获的分步说明，请参阅思科支持论坛文章：

嗅探器模式下的思科AP

对于使用无线客户端设备的漫游场景进行故障排除，常见挑战在于有效地收集跨多个信道的OTA数据包捕获。这种同时监控多个802.11信道的方法是通过收集汇聚的OTA数据包捕获来实现的。为此，建议使用多个兼容的802.11ac功能USB WLAN适配器与兼容的网络分析软件配合使用。一些常见的802.11ac功能USB WLAN适配器包括适用于OmniPeek的Savvius WiFI适配器(802.11ac)、Netgear A6210或类似产品。

十。总结

以下是需要收集的信息简要总结，以有效解决与CUWN的潜在无线客户端互操作性问题。本节旨在根据需要作为快速参考部分。

一、问题定义

- 此问题是否仅限于特定型号的接入点和/或无线电类型（2.4 GHz与5 GHz）？
- 是否仅在特定版本的无线局域网控制器(WLC)软件上观察到此问题？
- 仅客户端类型和/或软件（操作系统版本、WLAN驱动程序版本……）的特定版本遇到的问题
- 是否有其它无线设备不存在此问题？如果有，是什么问题？
- 当客户端连接到开放式SSID、信道宽度为20 MHz且禁用了802.11ac时，此问题是否可重复？（此问题是否发生在11n模式与仅11ac模式下）
- 如果问题在开放式SSID下无法再现，则至少会发现什么安全配置？（WLAN上的PSK或802.1X）
- 以前已知良好的配置和软件版本是什么？

二。 WLC配置和日志

从相关WLC的CLI收集此信息：

- config paging disable
- show run-config

或者，也可以根据需要仅收集以下输出：

- config paging disable
- show run-config no-ap
- show wlan apgroups

通过TFTP、FTP备份WLC配置……(GUI: **Commands > Upload File > Configuration**)

来自WLC的系统日志

三、客户端设备信息

- 客户端类型（平板电脑、智能手机、笔记本电脑……）
- 设备的品牌和型号
- 操作系统 版本
- WLAN适配器型号
- WLAN适配器驱动程序版本
- 使用的请求方（Windows零配置/自动配置、英特尔PROSet...）
- 为无线客户端和WLAN(Open、PSK、EAP-PEAP/MSCHAPv2、...)使用配置的安全性

  注意：任何客户端参数均更改了相关供应商提供的默认设置。（睡眠状态、漫游参数、U-APSD...）

四。网络拓扑图

这包括有关网络中无线设备的表示和/或详细信息（打印机/扫描仪、WLC、...）

V.创建电子表格记录所有客户问题

示例：

Mac地址	用户名	所报告症状的描述	最终用户观察到症状的时间	Ping默认网关Y/N	WiFi信号状态（已连接/正在

本练习的目标是帮助确定常见模式，并展示更准确地当前问题图景。

VI. WLC上的Show和Debug命令

通过CLI收集以下WLC调试：

- **配置会话超时0**
- debug client <MAC_address>
- debug dhcp message enable

逐个添加其他调试：

- debug aaa detail enable — 如果AAA服务器存在身份验证相关问题，请使用此命令
- debug aaa events enable — 如果AAA服务器存在身份验证相关问题，请使用此命令
- debug aaa all enable — 将其用于身份验证问题；这是详细的，因此仅在需要时使用（用于AAA覆盖情况等）
- debug mobility handoff — 在WLC之间的漫游问题时使用

通过CLI收集WLC show命令的输出：

- config paging disable
- show time
- show client detail <mac-address of client>（注意WLC上的客户端状态）

- 从WLC对客户端执行ping操作

测试完成后，使用此命令停止WLC上的所有当前调试：

- debug disable-all

七.AP上的show和debug命令

轻型Cisco IOS® AP

本节详细介绍1700/2700/3700系列或以前型号的接入点所需的调试。

要避免Telnet/SSH/控制台会话时AP会话超时，请使用以下命令：

- debug capwap console cli
- config t
- line console 0 — 用于修改串行会话超时参数
- line vty 0 4 — 用于修改Telnet/SSH会话超时参数
- exec-timeout 0
- 会话超时0
- term len 0

开始测试之前，请在AP上收集这些show命令的示例。在完成测试之前和之后，通过CLI使用以下AP show命令至少收集此输出的两个示例：

- term len 0
- show clock
- show tech
- show capwap client mn
- show int do1 dfs
- show logging
- more event.log
- show trace dot11_rst display time format local
- show trace dot11_rst
- show trace dot11_bcn display time format local
- show trace dot11_bcn

通过CLI收集以下AP调试：

- debug dot11 { d0 | d1 } monitor addr <MAC_address>
- debug dot11 { d0 | d1 } trace print clients mgmt keys rxev txev rcv xmt txfail ba
- 学期星期一

测试完成后，使用此命令可禁用调试：

- u all

AP-COS AP

本节详细介绍1800/2800/3800系列AP所需的调试。

要避免Telnet/SSH/控制台会话时AP会话超时，请使用以下命令：

- exec-timeout 0

在开始测试之前，收集AP上的show命令示例。在完成测试之前和之后，通过CLI使用以下AP show命令至少收集此输出的两个示例：

- term len 0
- show clock
- show tech
- show client statistics <client_MAC-address>
- show cont nss status
- show cont nss stats
- show log

对于1800系列接入点，通过CLI收集以下AP调试：

- debug dot11 client level events addr <client_MAC-address>
- debug dot11 client level errors addr <client_MAC-address>
- debug dot11 client level critical addr <client_MAC-address>
- debug dot11 client level info addr <client_MAC-address>
- debug dot11 client datapath eapol addr <client_MAC-address>
- debug dot11 client datapath dhcp addr <client_MAC-address>
- debug dot11 client datapath arp addr <client_MAC-address>
- **学期星期一**

对于2800/3800系列接入点，通过CLI收集以下AP调试：

- config ap client-trace address add <client_MAC-address>
- config ap client-trace filter all enable
- config ap client-trace output console-log enable
- config ap client-trace start
- **学期星期一**

测试完成后，使用此命令可禁用调试：

- config ap client-trace stop

八、客户端捕获

从客户端设备的WLAN适配器收集混合Netmon 3.4（仅限Windows XP或7）或Wireshark数据包捕获。

九。 OTA捕获

802.11n捕获

- 带Wireshark的AirPCAP
- MacBook Pro
- OmniPeek Professional、Enterprise、...
- OmniPeek远程助理(ORA)
- 嗅探器模式下的思科AP

802.11ac捕获

- 对于11ac 3SS捕获，您可以使用运行10.10.x或更高版本的2014 Macbook Pro或更高版本（如果可能，请勿将MacBook Air用于11ac捕获，因为它是当前仅支持2SS的设备）。
- 您也可以在嗅探器模式下使用2702、3702或类似的Cisco AP。
- 适用于漫游场景并使用专业网络分析软件，例如来自Savvius的OmniPeek。建议使用多个兼容802.11ac的USB WLAN适配器，例如适用于OmniPeek的Savvius WiFI适配器(802.11ac)、Netgear A6210或类似产品。

十一。附录A — 其他提示和诀窍

Windows 窗口版本

直接从Windows PC收集一些有关当前无线连接的其他信息以及其他相关详细信息。您可以在Windows命令行(CMD)中使用以下netsh wlan相关命令：

```
C:\Users\engineer>netsh wlan show ?
These commands are available:
Commands in this context:
show all       - Shows complete wireless device and networks information.
show allowexplicitcreds - Shows the allow shared user credentials settings.
show autoconfig - Shows whether the auto configuration logic is enabled or
                 disabled.
show blockednetworks - Shows the blocked network display settings.
show createalluserprofile - Shows whether everyone is allowed to create all
                 user profiles.
show drivers   - Shows properties of the wireless LAN drivers on the system.
show filters   - Shows the allowed and blocked network list.
show hostednetwork - Show hosted network properties and status.
show interfaces - Shows a list of the wireless LAN interfaces on
                 the system.
show networks  - Shows a list of networks visible on the system.
show onlyUseGPProfilesforAllowedNetworks - Shows the only use GP profiles on GP
configured networks setting.
show profiles  - Shows a list of profiles configured on the system.
show settings  - Shows the global settings of wireless LAN.
show tracing   - Shows whether wireless LAN tracing is enabled or disabled.
```

```
C:\Users\engineer>netsh wlan show interfaces
There are 3 interfaces on the system:

    Name                   : Wireless Network Connection 8
    Description            : WildPackets Conceptronic Nano Wireless 150Mbps USB
Adapter #5
    GUID                   : 6beec9b0-9929-4bb4-aef8-0809ce01843e
    Physical address       : c8:d7:19:34:d5:85
    State                  : disconnected

    Name                   : Wireless Network Connection 4
    Description            : WildPackets Conceptronic Nano Wireless 150Mbps USB
Adapter
    GUID                   : 23aa09d4-c828-4184-965f-4e30f27ba359
    Physical address       : 48:f8:b3:b7:02:6e
    State                  : disconnected

    Name                   : Wireless Network Connection
    Description            : Intel(R) Centrino(R) Advanced-N 6200 AGN
    GUID                   : 8fa038f8-74e0-4167-98f9-de0943f0096c
    Physical address       : 58:94:6b:3e:a1:d0
```

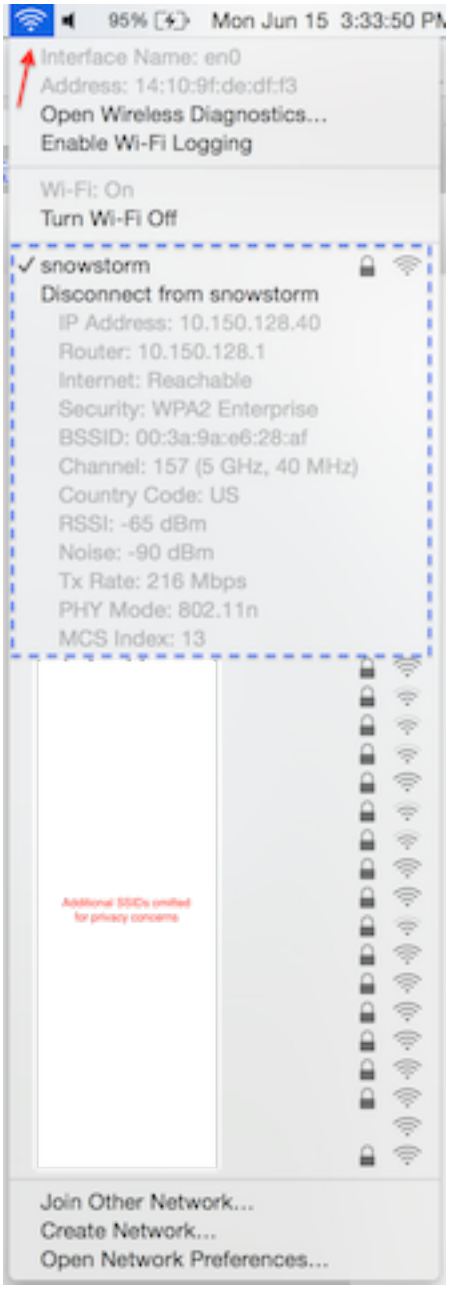
```
    State                   : connected
    SSID                    : snowstorm
    BSSID                   : 00:3a:9a:e6:28:af
    Network type            : Infrastructure
    Radio type              : 802.11n
    Authentication          : WPA2-Enterprise
    Cipher                  : CCMP
    Connection mode         : Profile
    Channel                 : 157
    Receive rate (Mbps)     : 300
    Transmit rate (Mbps)    : 300
    Signal                  : 80%
    Profile                 : snowstorm

    Hosted network status   : Not started


C:\Users\engineer>netsh wlan show networks bssid | more

Interface name : Wireless Network Connection
There are 21 networks currently visible.

SSID 1 : snowstorm
    Network type            : Infrastructure
    Authentication          : WPA2-Enterprise
    Encryption              : CCMP
    BSSID 1                 : 00:3a:9a:e6:28:af
         Signal             : 99%
         Radio type         : 802.11n
         Channel            : 157
         Basic rates (Mbps) : 24 39 156
         Other rates (Mbps) : 18 19.5 36 48 54
    BSSID 2                 : 00:3a:9a:e6:28:a0
         Signal             : 91%
         Radio type         : 802.11n
         Channel            : 6
         Basic rates (Mbps) : 1 2
         Other rates (Mbps) : 5.5 6 9 11 12 18 24 36 48 54

-- More  --
```

macOS（以前称为OS X）

为了在Windows PC上收集与**ipconfig /all**命令相同的输出，您可以改为使用常用的Linux/Unix命令**ifconfig**来列出Apple MacBook上所有网络接口的详细信息。根据需要，您还可以指定只接收给定MacBook的本地无线接口的输出（en0或en1，取决于型号）。如以下示例：

```
bash-3.2$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 14:10:9f:de:df:f3
inet6 fe80::1610:9fff:fede:dff3%en0 prefixlen 64 scopeid 0x4
inet 10.150.128.40 netmask 0xffffe000 broadcast 10.150.159.255
nd6 options=1<PERFORMNUD>
media: autoselect
status: active
```

为了快速获取有关MacBook上当前无线连接的一些详细信息。您还可以选择桌面右上角的WiFi图标，同时按住键盘上的**选项**按钮（如图所示）。



另一个有用的选项是使用隐藏的命令行实用程序airport。强烈建议仅将此功能与您自己的MacBook或实验室环境中正在使用的MacBook结合使用。由于某些网络管理员可能不希望授予对最终用户MacBook上此实用程序的访问权限，因此请相应地采取适当的注意级别。要继续，请在有问题的MacBook的Terminal中输入以下内容：

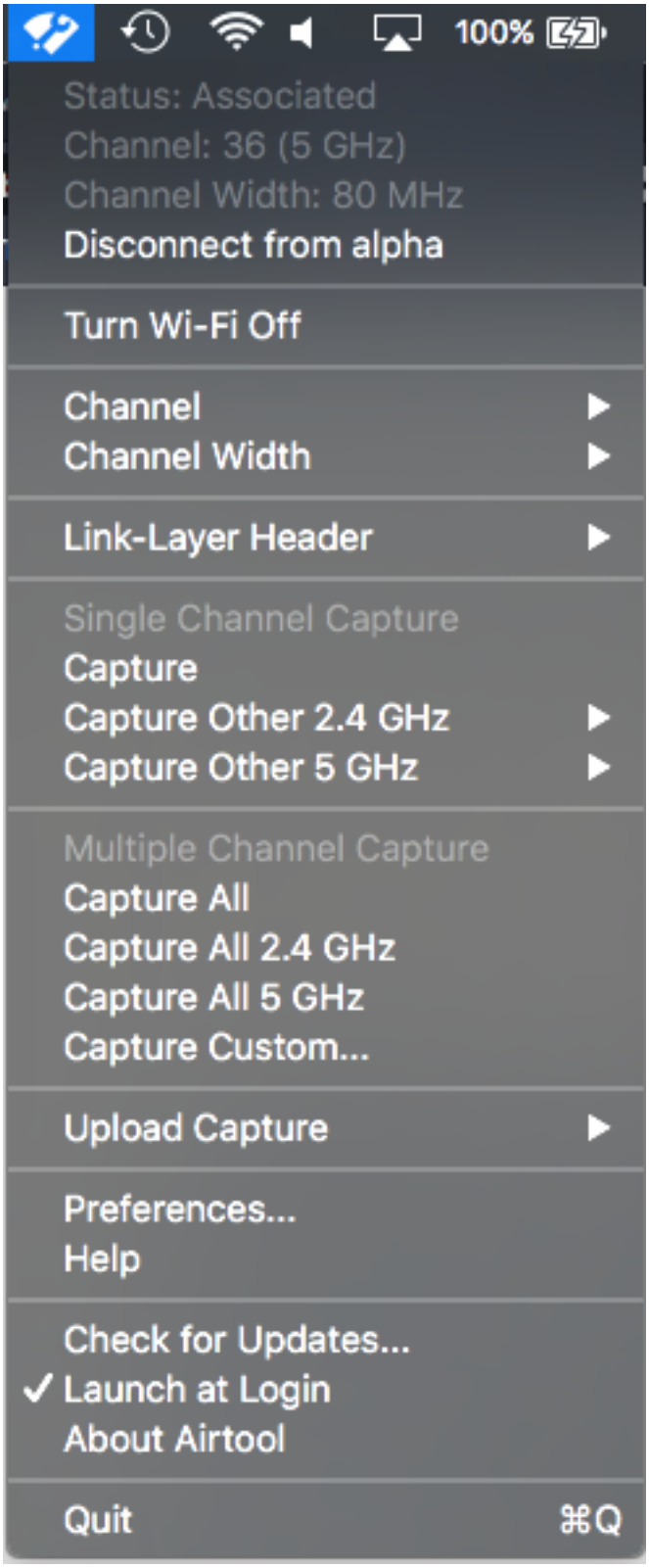
```
sudo ln -s
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
/usr/local/bin/airport
```

现在您可以轻松地调用机场CLI实用程序。例如：

```
bash-3.2$ airport -I
     agrCtlRSSI: -61
     agrExtRSSI: 0
    agrCtlNoise: -90
    agrExtNoise: 0
          state: running
        op mode: station
     lastTxRate: 216
        maxRate: 300
```

```
lastAssocStatus: 0
    802.11 auth: open
      link auth: wpa2
          BSSID: 0:3a:9a:e6:28:af
           SSID: snowstorm
            MCS: 13
        channel: 157,1
```

为进一步简化使用MacBook Pro或类似功能收集可靠的单个802.11信道OTA数据包捕获的流程。您可以使用Wireless Diagnostics > Sniffer方法或Wireless Diagnostics > Sniffer方法利用macOS中的嵌入式功能，也可以选择使用第三方实用程序Airtool（OS X 10.8及更高版本）。其优点是简单的界面可以快速收集OTA数据包捕获，只需从屏幕顶部的菜单栏中通过应用UI点击几下，即可将捕获的数据直接保存到桌面。



有关Airtool的更多信息和下载链接，请访问以下URL:

https://www.adriangranados.com/apps/airtool

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。